

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 3234 North Sydenham Street, Philadelphia, PA

Case No. 18-1653-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

See Attachments B, C

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

21 USC sec. 846

Offense Description

Conspiracy to distribute controlled substances

The application is based on these facts:

See Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Charles E. Simpson III, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

October 18, 2018



Judge's signature

City and state: Philadelphia, Pennsylvania

Honorable Carol S. Wells, US Magistrate Judge

Printed name and title

AFFIDAVIT

I, Charles E. Simpson, Special Agent, Federal Bureau of Investigation ("FBI"), Philadelphia, Pennsylvania, being duly sworn, state:

Introduction and Agent Background

1. I am an "investigative or law enforcement officer" as defined in 18 U.S.C. § 3051, as such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

2. I am a Special Agent (SA) with the FBI-Philadelphia Field Division. I have been employed by the FBI since April 2010. During my tenure with the FBI, I have been assigned to the High Intensity Drug Trafficking Area (HIDTA) / Safe Streets Violent Drug Gang Task Force (SSVDGTF) of the Philadelphia Division, which investigates, among other violations of federal law, violent drug gangs and criminal organizations including those involved in the importation, distribution and manufacturing of controlled substances, Hobbs Act violations, outlaw motorcycle gangs and homicides and shootings resulting from the drug trade. I have investigated numerous firearms violations, drug violations, and other related crimes. I have conducted physical and electronic surveillance, debriefed confidential sources, and participated in the drafting and execution of search warrants involving these matters. I am an active investigator for the FBI Gangs and Criminal Enterprise Program in which state and local arrests for drugs and firearms violations are reviewed and referred for possible federal prosecution.

3. I have participated in numerous narcotics investigations, debriefed or participated in debriefings of numerous of defendants, informants and witnesses who had personal knowledge regarding major drug trafficking organizations, and have participated in all aspects of drug investigations. I have participated in all aspects of narcotics investigations

including surveillance, analyzing information obtained from court-authorized pen register and trap and trace intercepts, Title-III wiretap investigations, and analyzing telephone toll records. I am aware that drug traffickers commonly use cellular telephones and other electronic devices in furtherance of their drug trafficking activities and frequently change cellular telephone numbers and cellular phones in an effort to thwart law enforcement's use of electronic surveillance.

4. This affidavit is submitted in support of a search warrant for:

a) Target Residence: 3234 North Sydenham Street, Philadelphia, PA 19140.

A two story row home located on the west side of the 3200 block of North Sydenham Street.

b) I am requesting authority to search the premises where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits and evidence of a crime.

c) I am also requesting authority to search all electronic devices seized inside the Target Residence as listed in Exhibit C.

5. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other special agents of FBI and other law enforcement; from my discussions with witnesses and confidential sources involved in the investigation; and from my review of records and reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another FBI special agent, law enforcement officer, witness or cooperating source who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are

stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein are not being relied on in reaching my conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of a violation of Title 21 United States Code, Sections 846 and 841(a)(1) (drug distribution conspiracy) will be found inside 3234 North Sydenham Street, Philadelphia, PA 19140 ("Target Residence"), as well as any electronic devices found therein.

B. THE INVESTIGATION AND PROBABLE CAUSE

7. This application is submitted in support of an FBI investigation into a drug trafficking organization, believed to operate primarily in Philadelphia with connections in California, Las Vegas, and various parts of the United States, including the Eastern District of Pennsylvania. This application seeks authority to search the Target Residence where AMIR BOYER and ABDUL WEST are believed to be carrying out drug trafficking activities.

8. Since March 2017, the FBI and the Philadelphia Police Department have been investigating a violent drug trafficking organization known as the Original Block Hustlaz (OBH) gang and several targets that are believed to be members of the organization, including ABDUL WEST, the leader of the OBH gang, and AMIR BOYER. The OBH gang is involved in drug trafficking and violence primarily in the Philadelphia area. Agents and Officers have conducted numerous controlled narcotics purchase operations from OBH members or subjects believed to be supplied by OBH members, as well as conducted numerous surveillance operations of

suspected narcotics transactions. OBH gang members also have a large social media presence which is monitored by the FBI. Much of the social media activity of the gang members discusses or suggests the ongoing illegal activities of the gang. Additionally, the Philadelphia FBI and the Philadelphia Police Homicide unit are currently investigating three homicides and three non-fatal shootings that are directly related to or carried out by members of the OBH gang. Specifically, investigators have evidence to believe that one of those homicides was carried out by an OBH gang member as part of a drug robbery. Drugs from that robbery were later sold to an FBI confidential informant and are currently evidence in the custody of the FBI.

9. On September 11, 2017, Philadelphia Police Officers executed a search warrant in furtherance of a homicide investigation of the Target Residence. Inside the Target Residence officers seized approximately 240 grams of heroin, 65 grams of crack cocaine, 52 grams of methamphetamine, and 1200 grams of marijuana. They also located and seized \$8,101.00 in United States Currency and a .45 caliber handgun. Shortly before police officers arrived to secure the residence for the search, FBI surveillance observed, via a pole camera, WEST and BOYER going into and out of the residence, and, at the time the police officers arrived, WEST and BOYER were in front of the residence.

10. Based on cell phone evidence collected from WEST, the members of the drug trafficking organization are believed to be using the Target Residence to store narcotics and/or US currency used during their drug trafficking operations. By way of example, on or about February 5, 2018, WEST and co-conspirator HANS GADSON used their cellular telephones to coordinate the exchange of narcotics and/or drug trafficking proceeds kept in a safe located inside the Target Residence.

11. On October 17, 2018, defendant AMIR BOYER was charged in a Superseding Indictment with violating the following statutes: Count One—conspiracy to distribute 5 kilograms or more of a mixture and substance containing a detectable amount of cocaine, 280 grams or more of a mixture and substance containing a detectable amount of cocaine base (“crack”), and 50 grams or more of methamphetamine, in violation of Title 21, United States Code, Section 841(a)(1), (b)(1)(A); Count Two—possession with intent to distribute 28 grams or more of a mixture and substance containing a detectable amount of cocaine base (“crack”), 100 grams or more of a mixture and substance containing a detectable amount of heroin, and approximately 48 grams of a mixture and substance containing a detectable amount of methamphetamine. Count Two of the Superseding Indictment is based on the September 11 seizure of narcotics at the Target Residence.

12. On October 17, 2018, the Honorable Carol S. Wells, United States Magistrate Judge, issued an arrest warrant for AMIR BOYER.

13. On October 18, 2018 at approximately 6:00 AM, Agents and Officers arrived at the Target Residence to arrest BOYER, who agents had observed coming into and going out of the Target Residence on October 16, 2018. Officers knocked and announced their presence. After a reasonable amount of time, BOYER did not answer the door and agents gained entry into the front door. BOYER was located at the top of the steps of the second floor and taken into custody. During a protective sweep of the Target Residence, officers opened a door that they believed lead to the basement of the house. The basement area was sealed off but sitting on the floor was a window unit air conditioner. On top of the window unit was a large black duffle style bag that was open on top. Protruding from the top of the bag, officers observed a clear plastic bag containing a large amount of a green leafy substance, believed to be

marijuana. Investigators believe it is likely the bag and the residence contain additional evidence related to the ongoing investigation.

C. METHODS OF NARCOTICS TRACKICKERS

14. Based on your affiant's training and experience, your affiant is aware that drug traffickers often use multiple cellphones and maintain books, records, receipts, notes, ledgers, passports, airline tickets, money orders and/or other papers relating to their travel and transportation, ordering, sale and distribution of drugs; that drug traffickers commonly front (provide drugs on consignment) drugs to their clients; that the aforementioned cellphones, books, records, ledgers, etc. are maintained where the drug traffickers have ready access to them including their residences and vehicles they are using to conduct their drug trafficking business. Further, I know that indicia of occupancy, residency and ownership of premises, including but not limited to utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents and keys are often maintained at such drug trafficking locations.

15. Narcotics traffickers commonly conceal in their residences, businesses, and automobiles large quantities of currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds from such illegal activities as well as evidence of financial transactions relating to obtaining, transferring, secreting, or spending large sums of money obtained from such illegal activities. Despite these attempts at concealment, it is not uncommon for narcotics traffickers to maintain photographs of persons or places associated with their illegal activities.

16. When narcotics traffickers amass proceeds from the sales of narcotics, those persons often attempt to legitimize these profits or otherwise conceal them from discovery by

law enforcement officers. To accomplish those goals, narcotics traffickers often use different techniques including, but not limited to, the use of foreign and domestic banks and their attendant services, securities, cashier's checks, money orders, money drafts, letters of credit, brokerage houses, the purchase of real estate, as well as shell corporations and business fronts to conceal the true ownership and illegal source of the proceeds. Further, records and documentary evidence of such financial transactions are frequently maintained in electrical, electronic, or magnetic form (such as information on a computer or cellular telephone).

17. Based on your affiant's training and experience, your affiant is aware that drug traffickers frequently possess firearms and other weapons at the premises where they conduct drug trafficking or in vehicles used to conduct drug transactions. Persons who traffic in drugs often maintain at their residences and other locations where they conduct drug trafficking activities unsold or undistributed supplies of controlled substances and other drugs, as well as the drug paraphernalia including chemical dilutents, weighing scales, mixing bowls, glassine bags, spoons, which are utilized in the weighing and packaging of controlled substances needed to be used to break down drugs into smaller quantities for distribution.

18. Based on your affiant's training and experience, your affiant is aware that drug traffickers often store large amounts of money they have amassed through their narcotics trafficking activities at their residences or residences owned/rented by family members or girlfriends or in the vehicles they are using for drug trafficking activities. In addition, I am aware based on my training and experience that drug traffickers also store large amounts of money that they have amassed in their narcotics trafficking activities at certain residences they believe are not known to law enforcement in order to avoid the money being seized by law enforcement.

19. Based on your affiants training and experience, your affiant is aware that

individuals involved in drug trafficking often use multiple cellphones, including but not limited to blackberries, smart phones or PDAs to store the telephone numbers for their drug trafficking associates. I am aware that those involved with drug trafficking often keep old cellphones at their residences to allow the individuals to restore contacts into newer cellphones.

20. Based on your affiant's training and experience, your affiant is aware individuals involved in drug trafficking often maintain more than one phone or more than one SIM card device, in order to have multiple avenues to facilitate drug trafficking activities, and in an attempt to avoid detection by law enforcement. I am aware that individuals involved in drug trafficking often times utilize pre-paid cellular telephones which do not maintain specific subscriber information, and/or use phones subscribed to in the name of third person, in order to mask their direct linkage to telephones utilized in furtherance of drug trafficking activities. Further, those involved in drug trafficking often change SIM cards in order to make it difficult for law enforcement to determine their records. Based on my training and experience, as well as the training and experience of other agents, I know that individuals involved in drug trafficking also frequently switch telephone numbers and/or phones. Despite the constant switching of active telephone numbers, drug traffickers often keep old phones.

21. Based on your affiant's training and experience, your affiant is aware that drug traffickers commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, I know that drug traffickers often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

22. Specifically, I know that those involved in drug trafficking communicate with

associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know those involved in drug trafficking communicate with associates using cellular telephones and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

23. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific traffickers.

24. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. I am also aware that drug traffickers often take photographs or make videos of drugs and drug proceeds with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

25. Furthermore, based on your affiant's training and experience, your affiant is aware that drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use an Internet search engine to explore where banks or mail delivery services are located, or may use the Internet to make reservations for drug-related travel. In addition, I know that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators, and to display drugs and drug proceeds or to post photographs of locations where they have traveled in furtherance of their drug trafficking activities.

26. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

27. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

28. Based drug on my training and experience, I know that indicia of occupancy,

residency and the rental and/or ownership of premises, including but not limited to utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents and keys are often maintained in vehicles used by such individuals. Furthermore, I know that drug traffickers commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their financial and business transactions. For example, I know that they often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

29. Based on my training and experience, I know that individuals involved in drug trafficking often use multiple cellphones, including but not limited to blackberries, smart phones or PDAs to store the telephone numbers for their drug trafficking associates. I also know that individuals involved in drug trafficking maintain telephone numbers and other information on their cell phones. I am aware that those involved with drug trafficking often keep old cellphones in close proximity to allow them to restore contacts into newer cellphones.

30. Specifically, I know that those involved in drug traffickers communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they may leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know they also communicate with associates using cellular telephones and tablets to send e-mails and text messages and communicate via social media networking sites. By analyzing call and text communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates

during the commission of the crimes.

31. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific traffickers.

32. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. I am also aware that drug traffickers often take photographs or make videos of drug proceeds with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

33. Furthermore, based on my training and experience, and the training and experience of other agents, I know that drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their criminal activities. Specifically, drug traffickers may use an Internet search engine to explore where banks or other financial services are located, or may use the Internet to make reservations for criminally-related travel. In addition, I know that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators.

34. In addition, drug traffickers sometimes use cellular telephones as navigation

devices, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

35. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

D. ELECTRONIC DEVICES

36. This application also seeks permission to search and seize electronic devices, including cellular telephones, for evidence described in Attachment C. As used herein, the term “electronic device” includes any electronic system or device capable of storing or processing data in digital form, in this case referring specifically to wireless or cellular telephones.

37. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices. In particular, I know that electronic devices, including cellular telephones used by drug traffickers, are likely to be repositories of evidence of crimes. I know that an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and

received, and other records that may indicate the nature of the offense.

38. Furthermore, I know that electronic devices, such as cellular telephones, can store information for long periods of time. Examples of such information include text and multimedia message conversations, call history, voice mail messages, e-mails, photographs, and other data stored on the device. Similarly, I know from my training and experience that when cellular telephones are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

39. Based on my experience and training, as well as the experience and training of other agents, I know that even when a user deletes information from a device, it can sometimes be recovered with forensics tools.

40. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that searching electronic devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of electronic devices and software programs in use today that specialized equipment is sometimes necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of electronic devices, operating systems, or software applications that are being searched.

41. Furthermore, I am aware that electronic data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching electronic devices can require the use of precise, scientific procedures that are designed to maintain the integrity of electronic data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a

result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on electronic devices.

42. Also, I know from my training and experience that the volume of data stored on many electronic devices will typically be so large that it will often require a search of the device in a law enforcement laboratory or similar facility. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

43. I am also aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically

maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

44. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), electronic devices can contain other forms of electronic evidence as well. In particular, records of how an electronic device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the electronic devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the electronic device was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a

crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

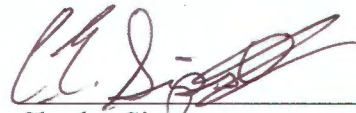
45. Further, evidence of how an electronic device has been used, what it has been used for, and who has used it, may be the absence of particular data on an electronic device. For example, to rebut a claim that the owner of an electronic device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the electronic device remotely is not present on the electronic device. Evidence of the absence of particular data on an electronic device is not segregable from the electronic device. Analysis of the electronic device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

46. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be co-mingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the FBI

intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B. In addition, given that the affidavit is in support of the search of electronic devices recovered during the execution of an anticipatory search warrant of the Target Residence, and these electronic devices will be then be stored as evidence with the FBI, there exists reasonable cause to permit the execution of a search of the seized electronic devices at any time in the day or night.

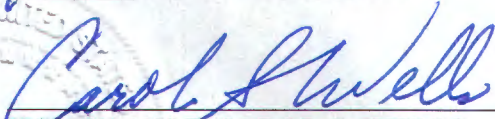
E. CONCLUSION

Based on the foregoing facts, your affiant believes that there is probable cause that the fruits and/or evidence of crimes specifically, violations of Title 21, United States Code, Sections 846, 843 and 841, as enumerated in Attachment B, will be found in the Target Residence, as well as in any electronic devices recovered inside the residence. Accordingly, I respectfully request that the Court issue a warrant to search the Target Residence as well as any electronic devices recovered therein.



Charles Simpson
Special Agent
Federal Bureau of Investigation

Sworn to before me this on this
18th day of October, 2018



HONORABLE CAROL S. WELLS
UNITED STATES MAGISTRATE JUDGE

Attachment A

Target Residence: 3234 North Sydenham Street, Philadelphia, PA 19140. A two story red brick row home located on the west side of the 3200 block of North Sydenham Street.



Attachment B

The following items constitute evidence of the commission of a violation of 21 U.S.C. Sections 846 and 841(a)(1), contraband, items unlawfully possessed, or property designed or intended to be used or which has been used as the means for committing such violations, and are located inside the Target Residence, as described in Attachment A:

1. Any and all United States currency, money counters and any item used in the counting of currency.
2. Books, records, receipts, notes, ledgers, passports, airline tickets, money orders and other papers related to travel and transportation, ordering sale and distribution of drugs
3. Cellular telephones, smart phones, tablets, computers or PDAs for any and all stored electronic communications, including but not limited to telephone or address directory entries consisting of names, addresses, telephone numbers, logs of telephone numbers dialed, telephone numbers of incoming, outgoing or missed calls, text messages, schedule entries, stored memoranda, videos, digital photographs, emails accounts and logs of website's visited.
4. Any and all business records, including but not limited to accounts receivable, accounts payable, general ledgers, cash disbursement ledger, check register, employment records, and correspondence, regardless of the identity of the person(s) involved in the transactions.
5. Any and all identification records and documents, including but not limited to birth certificates, state identification cards, social security cards, and driver's licenses.
6. Any and all banking records, including but not limited to monthly savings and

checking statements, canceled checks and banking communications, deposit tickets, withdrawal receipts, certificates of deposits, pass-books, money drafts, money orders (blank or endorsed), check cashing logs, wire transfer logs, cashier's checks, bank checks, money orders, safe deposit box keys, safes, money wrappers and wire transfers.

7. Indicia of occupancy, residency, and ownership or use of the subject premises, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents and keys.
8. Controlled substances, drug paraphernalia, including but not limited to, chemical dilutants, weighing scales, mixing bowls, glassine bags, spoons, utilized in the weighing and packaging of controlled substances.
9. Firearms and other weapons, and ammunition.

ATTACHMENT C

This warrant authorizes the search of electronic devices for the below-listed evidence of, or property designed for use, intended for use, or used in committing the distribution of and possession with intent to distribute controlled substances, in violation of 21 U.S.C. § 846:

- a. Electronic communications relating to the criminal activity,
- b. Telephone or address directory entries consisting of names, addresses, telephone numbers; logs of telephone numbers dialed, telephone numbers of incoming, outgoing or missed calls, text messages, schedule entries, stored memoranda, videos, social networking sites and digital photographs,
- c. Lists of customers and related identifying information,
- d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions,
- e. Any information related to sources of controlled substances, including names, addresses phone numbers, and any other identifying information,
- f. Any information related to the methods of trafficking in controlled substances;
- g. Any information recording domestic and international schedule or travel related to the described criminal activity, including any information recording a nexus to airport facilities, airport security, or airlines,
- h. All bank records, checks, credit cards, credit card bills, account information, and other financial records,
- i. Any information related to package delivery services, including but not limited to United States Postal Service, Federal Express and UPS,
- j. All data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system,

- k. Stored memoranda; stored text messages; stored electronic mail; stored photographs; stored audio; and stored video,
- l. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software,
- m. Evidence of the attachment of other devices,
- n. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device,
- o. Evidence of the times the device was used,
- p. Passwords, encryption keys, and other access devices that may be necessary to access any of the devices,
- q. Records of or information about Internet Protocol addresses used by the device,
- r. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "Favorite" web pages, search terms that the user entered into any Internet search engine, and records or user-typed web addresses, as well as evidence of the posting of videos, photos, or any material relevant to these crimes to any social networking site.
- s. Evidence of user attribution showing who used or owned the electronic devices at the time the things described above were created, edited, or deleted, such as logs phonebooks, saved usernames and passwords, documents, and browsing history.